UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

MARK MARMILEV,
a/k/a "Marko,"
a/k/a "Mark Halls,"

Defendant.

13 Cr. 368-2 (DLC)

GOVERNMENT SENTENCING SUBMISSION

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for the United States
of America

SERRIN TURNER
ANDREW D. GOLDSTEIN
CHRISTINE I. MAGDO
KEVIN MOSLEY
Assistant United States Attorneys

- Of Counsel -

**U.S. Department of Justice**

*United States Attorney*
*Southern District of New York*

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

December 9, 2014

By ECF and Hand Delivery
Hon. Denise L. Cote
United States District Judge
Daniel Patrick Moynihan United States Courthouse
500 Pearl Street
New York, New York 10007-1312

**Re: *United States v. Mark Marmilev*, 13 Cr. 368-2 (DLC)**

Dear Judge Cote:

The Government respectfully submits this sentencing letter in connection with the sentencing scheduled for December 12, 2014, of defendant Mark Marmilev, who was the chief technology officer of Liberty Reserve and a longtime associate of its founder, Arthur Budovsky. On September 11, 2014, Marmilev pled guilty to conspiring to operate a money transmitting business that failed to comply with federal registration requirements in violation of 18 U.S.C. § 1960(b)(1)(B) and that involved the transmission of funds that Marmilev knew were derived from or intended to be used to promote criminal activity, in violation of 18 U.S.C. § 1960(b)(1)(C). Pursuant to a plea agreement, the parties have stipulated that the Sentencing Guidelines call for a sentence at the statutory maximum – 60 months' imprisonment – which Probation recommends. But for that statutory cap, the parties have stipulated that Marmilev would face a Guidelines range of 135 to 168 months' imprisonment, based principally on the hundreds of millions of dollars that Liberty Reserve transmitted for U.S. customers without a federal license.

As set forth below, a Guidelines sentence is amply warranted in this case, based on two independent grounds. First, Marmilev was centrally involved in operating a business, Liberty Reserve, that transmitted an enormous volume of funds without a federal license, even though he had previously been involved in operating a similarly unlawful business, run by the same people, that was shut down by law enforcement authorities. Second, Marmilev knew – or at least had strong reason to believe – that Liberty Reserve was extensively used to process payments for criminal websites, and that, as Marmilev himself put it at one point, Liberty Reserve was "tolerant" of these "shady businesses." Based on these facts – which, despite Marmilev's attempts to muddy the factual waters, are not meaningfully contested – a Guidelines sentence is

clearly appropriate under 18 U.S.C. § 3553(a), in light of the seriousness of the offense, as well as the need for both general and specific deterrence.

## FACTUAL BACKGROUND

The section below tracks the facts set forth in the Presentence Report ("PSR") prepared by Probation. As the PSR notes, Marmilev has objected to a number of the facts contained in the PSR, although many of these objections, upon closer inspection, concern what inferences should be drawn from the facts set forth in the PSR, as opposed to being objections to the underlying facts themselves. In any event, as set forth in the Discussion section of this submission, there are more than enough uncontested facts before the Court to warrant imposition of a Guidelines sentence. Accordingly, although the Government would be prepared to prove the facts set forth in the PSR at a *Fatico* hearing, the Government does not believe that such a hearing is necessary for the Court to impose sentence in this matter. *See United States v. Ghailani*, 733 F.3d 29, 54 (2d Cir. 2013) ("'[I]t is well established that a district court need not hold an evidentiary hearing to resolve sentencing disputes, as long as the defendant is afforded some opportunity to rebut the [g]overnment's allegations.'") (quoting *United States v. Broxmeyer*, 699 F.3d 265, 280 (2d Cir. 2012) (internal quotation marks omitted).[1]

### Overview

Originally created in or about 2002 in Brooklyn, New York, and eventually moved offshore to Costa Rica in or about 2009, Liberty Reserve S.A. ("Liberty Reserve") operated one of the world's most widely used digital currencies, until it was indicted in this matter for money laundering and operating an unlicensed money transmitting business, in 2013, resulting in the arrests of its principals and the seizure of its website.

Arthur Budovsky, a/k/a "Arthur Belanchuk," a/k/a "Eric Paltz" was the principal founder of Liberty Reserve. At all relevant times, Budosvky directed and supervised Liberty Reserve's operations, finances, and corporate strategy. Vladimir Kats was a co-founder of Liberty Reserve along with Budovsky. Kats helped run Liberty Reserve until Budovsky forced him out of the company in or about 2009. Kats also operated multiple Liberty Reserve "exchanger" services.

As described further below, Marmilev began working for Budovsky and Kats in or about 2003, designing and maintaining websites for Budovsky and Kats' online businesses, including Liberty Reserve. Over time, Marmilev played an increasingly important role in operating Liberty Reserve, becoming, in essence, its Chief Technology Officer, responsible for overseeing

[1] Nor has the defendant moved for a *Fatico* hearing, despite the objections he raises to the PSR. "This course of conduct is not surprising. A defendant may well try to minimize his guilt by raising objections to unfavorable information in a PSR, while still trying to avoid any appearance of a false denial that could result in his losing acceptance of responsibility consideration, receiving an enhancement for obstruction of justice, or otherwise aggravating his sentence. Those same concerns will often prompt him not to pursue a hearing . . . ." *Broxmeyer*, 699 F.3d at 279 (finding defendant to have waived any right to a *Fatico* hearing under such circumstances).

its online and technical infrastructure. By 2010, Budovsky gave Marmilev a thirty-percent ownership share of Liberty Reserve. Marmilev personally received well over $1 million in proceeds from Liberty Reserve during the course of his employment.

How Liberty Reserve Worked

Through its website, www.libertyreserve.com, Liberty Reserve provided its users with what it described as "instant, real-time currency for international commerce," which could be used to "send and receive payments from anyone, anywhere on the globe." Liberty Reserve also touted itself as the Internet's "largest payment processor and money transfer system," serving "millions" of people around the world, including hundreds of thousands of users in the United States. To use the Liberty Reserve digital currency, commonly referred to as "LR," a user first needed to open an account through the Liberty Reserve website. In registering, the user was required to provide basic identifying information, such as name, address, and date of birth.

However, unlike mainstream banks or online payment processors, Liberty Reserve did not require users to validate their identity information when opening an account. As a result, a criminal could easily open a Liberty Reserve account using identity information that was fabricated or stolen. *See* Ex. A (screenshots from opening of undercover account under the name "Joe Bogus" from "Completely Made Up City, New York, United States"). In fact, users commonly established Liberty Reserve accounts under blatantly fictitious names, often using names signaling the users were involved in criminal activity. The following are examples, among many:

| | | | |
|---|---|---|---|
| card biz | hack banks | hacker boss | hell hacker |
| carder boss | Hack Crew | Hacker Ccv | Master Carder |
| Carder Profit | hack good | Hacker Cvv | Oliver Hacker |
| Cardshopteam | hack great | Hacker lover | real hacker |
| cc carding fullz | Hack Lord | Hacker ME | Russia Hackers |
| ccv hacker | hack master | Hacker YOU | seller hacker |
| CooLHacK | hack more | hacker socker | Spamming Tools |
| Cyber Hacker | hack pro | hacking seller | tasty hacker |
| Devil Hack | hack them | Hacking Tools | viet hacker |
| Good Hacker | Hack Tools | hackings software | wise hacker |
| Great Hacker | hacker account | hackxx deephack | young carder |

Once a user established an account with Liberty Reserve, the user could then conduct LR transactions with other Liberty Reserve users through the Liberty Reserve website. That is, the user could receive transfers of LR from other Liberty Reserve accounts, and could likewise transfer LR from his own account to other users' Liberty Reserve accounts.

However, unlike with mainstream banks or online payment processors, a Liberty Reserve user could not fund his account by transferring money to Liberty Reserve directly. Nor could a Liberty Reserve user withdraw funds from his account directly. Instead, Liberty Reserve users were required to purchase and redeem LR by using third-party "exchangers." These exchangers were individuals or entities separate from Liberty Reserve who maintained direct financial

relationships with Liberty Reserve, buying and selling LR in bulk from Liberty Reserve in exchange for mainstream currency. The exchangers in turn would buy and sell this LR in smaller transactions with end users in exchange for mainstream currency.

In order to fund a Liberty Reserve account, a Liberty Reserve user was required to transmit mainstream currency to an exchanger of the user's choosing. Upon receiving the user's payment, the exchanger credited the user's Liberty Reserve account with a corresponding amount of LR, by transferring LR from the exchanger's Liberty Reserve account to the user's Liberty Reserve account. If a Liberty Reserve user wished to withdraw funds from his account, the user was required to transfer LR from his Liberty Reserve account to an exchanger's Liberty Reserve account, and the exchanger then would make arrangements to send the user a corresponding amount of mainstream currency.

Because transferring money through the system entailed moving money through multiple financial institutions or money transmitting businesses, there were several separate fees that users incurred. First, to send real currency to a Liberty Reserve exchanger (for the exchanger to convert into Liberty Reserve), a user would typically have to send the money through a bank, or a money transmitter such as Western Union, which would charge a fee for the transfer. Second, the Liberty Reserve exchanger would then charge the user for exchanging the user's currency for LR and sending the LR to the user's Liberty Reserve account. These fees would typically be high – amounting to five percent or more of the funds being exchanged. Finally, once the LR was in the user's Liberty Reserve account, Liberty Reserve would charge the user a fee for any transfer the user made from his account to any other user's LR account. In order for the other LR user to convert the funds received back into real currency, that user too would have to pay a series of fees – to Liberty Reserve, and then to an exchanger – in order to cash out the funds. Accordingly, moving significant amounts of money through Liberty Reserve tended to be more cumbersome and expensive than moving money through traditional financial institutions. (*See* Ex. B (summary table showing accumulation of fees involved in undercover transfers into and out of Liberty Reserve)).

Liberty Reserve User and Transaction Statistics

Liberty Reserve had millions of user accounts and processed billions of dollars in user transactions.[2] According to data obtained from the company's computer servers, which were seized during the Government's investigation, Liberty Reserve had approximately 5.1 million user accounts as of May 2013. The total volume of transactions for all 5.1 million accounts reflected in the data (including payments sent and received from each account) is approximately $16.4 billion.

The Liberty Reserve transactional data also reflects that many of its users appear to have been based in the United States. Of the 5.1 million total user accounts contained in the transactional database, approximately 3.8 million accounts have country-of-origin data

[2] This figure does not necessarily represent the number of actual customers, however, as nothing prevented a customer from establishing multiple, indeed many, different accounts on Liberty Reserve's system.

associated with them, indicating that the users who registered these accounts provided a certain country of origin during the registration process. (This information was not verified by Liberty Reserve, however.) Of those 3.8 million accounts, accounts from the United States compose 601,000, or 15.62% of the total number of Liberty Reserve accounts. The transaction volume associated with these U.S.-based Liberty Reserve accounts (incoming and outgoing payments) totaled more than $2.03 billion – constituting approximately 12.4% of the $16.4 billion in total transaction volume for all Liberty Reserve user accounts.

The Liberty Reserve transactional data also reflect transactions with accounts registered as "exchanger" accounts with Liberty Reserve. These were Liberty Reserve users that were designated on Liberty Reserve's system as exchangers authorized to convert users' real currency to LR and vice-versa. (Many "underground" exchangers also operated on Liberty Reserve but were not designated as exchanger accounts on its system.) The data for these exchanger accounts reflect outgoing transfers of LR to U.S.-based users totaling approximately $114 million. These transfers correspond with purchases of LR by U.S.-based users in exchange for real currency. The data for the exchanger accounts likewise reflect incoming transfers of LR from U.S.-based users totaling approximately $95 million, corresponding with cashouts of LR by U.S.-based users through these exchangers. In short, the total amount of money transferred in and out of the Liberty Reserve system by U.S.-based users, through designated Liberty Reserve exchangers, was approximately $209 million.

This $209 million figure is included in the plea agreement between the Government and Marmilev as the value of the funds involved in the offense. It is a conservative estimate that does not reflect the approximately $1.81 billion in transactions on Liberty Reserve's system that U.S.-based users engaged in with other Liberty Reserve users (*i.e.*, users other than those designated as exchangers).

Failure to Register as Money Transmitting Business under Federal Law

Under Title 18, United States Code, Section 1960, it is a felony to conduct a "money transmitting business" if, among other things, the business is not registered as a money transmitting business with the Secretary of the Treasury as required under Title 31, United States Code, Section 5330 or regulations prescribed thereunder, or if the business otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or intended to be used to promote unlawful activity. *See* 31 C.F.R. §§ 1010.100(ff)(5), 1022.380(a)(2).

The implementing regulations for Title 31, United States Code, Section 5330 specifically apply to foreign-based money transmitting businesses doing substantial business in the United States. *See id*. As noted above, at least 600,000 Liberty Reserve accounts, which engaged in more than $2 billion in transactions on Liberty Reserve's system, are associated with users who reported their country of origin as the United States. Notwithstanding that Liberty Reserve thus did substantial business with customers in the United States, at no time did the company ever register with the United States Department of Treasury as a money transmitting business.

Criminal Use of Liberty Reserve

The Government's investigation uncovered a wide variety of evidence reflecting the extensive use of Liberty Reserve by criminal users – in particular, criminal websites or online schemes that used Liberty Reserve to receive payments from their customers or victims or to launder the proceeds of their illegal enterprises. By contrast, the Government's investigation uncovered no evidence of substantial use of Liberty Reserve by legitimate, mainstream online businesses (such as Amazon.com or other online shopping venues).

*Liberty Reserve's featured "merchants."* The Liberty Reserve website itself featured a list of links to some of the "merchant" webpages where users could spend their LR. (*See* Ex. C (screenshot of Merchants webpage)). As of May 2013, only two links to "merchants" were featured under the category "Shopping." One link led to a Facebook page of an individual in Indonesia offering to "resell" a seemingly random collection of clothing, electronics, and other goods, consistent with fencing stolen merchandise. The second link led to www.kupitam.com ("Kupitam"), a site which Vladimir Kats participated in operating and which allowed a user to specify any item on the Internet that the user wished to purchase (for example, an item for sale at Amazon.com). Kats would then purchase the specified item for the user. After the item was delivered to Kats, Kats would re-ship the item to the user, in exchange for payment in LR. The website charged high "processing" fees that would deter anyone from using the site for legitimate business activity. (*See* Ex. D (screenshot of website and documentation of undercover purchase of Apple keyboard)). Instead, the site enabled Liberty Reserve users to purchase goods from mainstream vendors – who otherwise would not accept such form of payment – and to do so indirectly, so as to avoid leaving a record of their identities or shipping locations with the vendors.

Other "merchants" featured on the Liberty Reserve website were likewise clearly oriented toward criminal clients. One website, www.ptshamrock.com ("PTShamrock"), listed under the category "Finance," offered offshore banking services and brazenly claimed to be able to provide its clients with the means to obtain driver's licenses, passports, and even appointments to ambassadorial or consular positions in certain countries. (*See* Ex. E (screenshot of PTShamrock website)). Most of the other "merchants" featured on the Liberty Reserve website were listed under the category "Internet Services," and provided web "privacy" or "security" services, such as virtual private networks, encryption, and "offshore" website hosting (*i.e.*, hosting of websites on servers located in jurisdictions with weak or lax law enforcement systems). Such services are frequently used by online criminals to hide their tracks or to otherwise prevent detection or disruption of their criminal activity by law enforcement.

*Google Analytics Data.* Liberty Reserve used various tools to monitor user traffic on its website. One of the tools it used was Google Analytics. Google Analytics is a service operated by Google, Inc, which caters to online businesses. A business subscribed to Google Analytics (the "subscriber") can use the service to monitor traffic to and within the subscriber's website. Google Analytics collects information about a website's users by installing a "cookie" – a small piece of data – on the computer of each user of the subscriber's website. The "cookie" collects information about the user's interactions with the website, by, for example, tracking what pages of the subscriber's website the user visits.

Among the user data collected by Google Analytics is "referral traffic," which lets the subscriber see what websites are referring traffic to the subscriber's website – that is, the websites that users are visiting immediately before visiting the subscriber's website. Such data can help the subscriber understand the sources of its online business. (For example, if the subscriber operates a website selling sports equipment, "www.sportsequipment.com," and advertises on various sports-related websites, the subscriber can use Google Analytics to see how much of the traffic to "www.sportsequipment.com" comes from the websites where the subscriber's site is advertised.)

Liberty Reserve offered online "merchants" using its services the ability to access Liberty Reserve through a shopping cart interface ("SCI"). In this way, the "merchants" could accept Liberty Reserve payments from customers directly on their own websites, without requiring the customers to log on separately to Liberty Reserve (just as many mainstream online merchants accept payments through Paypal). Data obtained from Google Analytics include the referral data for Liberty Reserve's SCI interface – *i.e.*, data reflecting the websites using Liberty Reserve's SCI interface to accept payment from their customers. Each referral reflects the use of Liberty Reserve to effectuate a payment for a transaction on the referring website.

Of the top ten websites that referred traffic to Liberty Reserve's SCI interface from 2007 to 2013 (in terms of volume of referrals), half of the sites were "carding" websites, *i.e.* websites engaged in trafficking stolen credit card data and related illegal goods and services.[3] In addition, the Google Analytics data reflects user traffic from hundreds of other carding websites – including 834 websites with domain names containing the word "card," such as "carder007.net" and "cardshop.tv" – and 487 other websites with domain names containing "cvv" such as "cvvshop.su" and "freshcvv.cc."[4]

Others websites included in the top ten sources of traffic to Liberty Reserve's SCI interface include offshore gambling sites, an Internet "proxy" service (hidemyass.com) often used by cybercriminals to conceal their identities online, and unregulated foreign exchange-trading platforms, which are known to be prominent sources of online fraud.[5]

---

[3] The top ten sites are, in descending order: validshop.su (carding site), secure.instaforex.com (forex), justbeenpaid.com (HYIP), exness.com (forex), miladccshop.biz (carding site), codeshop.su (carding site), miladdccshop.com (carding site), hidemyass.com (proxy site), pawn-shop.cc (carding site), planetofbets.com (offshore gambling site).

[4] The "cvv," or "card verification value" is the three or four digit security code on credit cards used to verify that the user of a card is in physical possession of the card. Carder sites can also be identified by the presence in the name of the website of various iterations of the term "dumps," and/or iterations of the term "fullz."

[5] *See* Commodity Futures Trading Commission, "Commission Advisory: Beware of Foreign Currency Trading Frauds," *available at* http://www.cftc.gov/opa/enf98/opaforexa15.htm. As explained in the advisory, unregulated websites offering individuals the opportunity to make money through foreign exchange trading are often forms of "high-yield investment programs" or "get rich quick" schemes. By contrast, mainstream international currency swap markets typically operate on government-regulated exchanges and are associated with traditional

*Data from Liberty Reserve Servers*. Data obtained from Liberty Reserve's servers similarly confirms the widespread use of the company's payment system by criminal websites. For example, the servers contain a database table called "Admin-Merchant.store," containing information about "merchants" operating on Liberty Reserve's system, including their user account number, username, and website address. The criminal nature of many of these merchants is self-evident, as reflected, for example, in the entries for the following carding websites:

| | | |
|---|---|---|
| U8498784 | best-carders | http://best-carders.ru/status.html |
| U7744687 | carder | http://store.carder.tw/paygates/lrstatus.php |
| U7164285 | V-carder | mailto:webmaster@v-carder.ws |
| U4537280 | iCarder CCstore | http://icarder.ru/lrstatus.php |
| U8637018 | carder | http://carder.vc/lrstatus.php |
| U4526232 | cardersmart | mailto:blackrauf@gmail.com |
| U9942053 | True-Carders | mailto:hackingxp@btopenworld.com |
| U7866662 | CarderShop | http://cardershop.biz/lrstatus.php |
| U3072736 | V-carder | mailto:webmaster@v-carder.ws |
| U4760486 | iCarder store | http://icarder.com/lrstatus.php |
| U7137263 | Carder2012 | mailto:carder2012@gmail.com |
| U8496272 | CarderShop | http://cardershop.com |
| U2562553 | carders3 | mailto:ali4000535@gmail.com |
| U4152006 | BlackCvv | http://blackcvv.com/shop/index.php?view=status |
| U5640371 | cvv2autoshop | http://cvv2autoshop.webs.com/ |
| U8843393 | Cvvstore | http://www.ccvstore.biz |
| U9358069 | isellcvv | http://www.cvvhost.com/lrstatus.php |
| U5307527 | t2cvvshop | http://www.t2cvvshop.com/funds_status.php |
| U9303799 | cvv2.name | https://cvv2.name/billing/lrreport/success/ |
| U3164525 | freshcvvshopstore | mailto:ccvsellers@gmail.com |
| U1996742 | MonsterCvv | http://37.46.125.111/~monsterc/ |
| U3358016 | shop cvvus.ru | http://216.120.252.8/~cvvuscom/process.php |
| U8345364 | CVVPLAZA | mailto:carder@easy.com |
| U1802446 | topcvv | http://www.topcvv.net/status.php |
| U2297397 | LIVECVVSHOP | http://livecvv.ru/lrstatus.php |
| U3822155 | Good cvv | http://mattfeuter.com/process.php |
| U4977656 | CVVSHOP | http://fullcvvshop.com |
| U1690808 | storefreshcvv | mailto:shopandtuan@yahoo.com |
| U5003215 | cvvshops | http://cvvshops.net/index.php |
| U5342189 | providecvv82 | http://providecvv.com/modules/libertyreserve/status.p |
| U1521107 | cvvme | http://cvvme.net/ |

consumer and investment banking services. Liberty Reserve was not an accepted form of payment at any such mainstream international currency swap markets.

| | | |
|---|---|---|
| U0856302 | T@CVV | http://www.t2cvv.net/user/lr2add/status.php |
| U5995737 | CVV BANK | http://www.cvvbank.us/lrstatus.php |
| U7504714 | cvvmn | http://cvv.mn/lrstatus.php |
| U7453348 | Online Shop CVV | mailto:ranicani@yahoo.com |
| U1253155 | Good cvv | mailto:malhotragaurav55@gmail.com |
| U8692716 | cvvlicom | http://cvvli.com/lrstatus.php |
| U1357912 | CvvPrivate | http://hauvuong.com/shop/process.php |
| U1427375 | sellcvv24h | http://sellcvv24h.com/modules/libertyreserve/status.p |
| U3762097 | cvv2.cc | http://176.31.220.185/gateway/lrstatus/ |
| U0962182 | CVV PRIDE | http://www.bnp-bicici.com |
| U9471516 | dumpscvv | http://www.dumpcvv.me/home.htm |
| U7270525 | cvv market | http://www.cvvmarket.bz/user/lr2add/status.php |
| U3762097 | cvv2.name | http://176.31.220.185/gateway/lrstatus/ |

Further, analysis of the top approximately 500 accounts by transaction volume, *i.e.* funds sent and received, indicates that a substantial amount of the activity in the Liberty Reserve system can be traced back to likely criminal activity. The total transaction volume for these accounts is approximately $7.2 billion, or 44% of the total volume of transactions on Liberty Reserve's entire system. Of these top approximately 500 accounts, 117 of the accounts, accounting for approximately $1.4 billion in transactions, were associated with online Ponzi schemes known as "high yield investment programs" or "HYIPs." Another 73, accounting for approximately $1.2 billion in transactions, were associated with unregulated "forex" (foreign currency trading) websites, and 32, accounting for approximately $210 million in transactions, were associated with trafficking in stolen credit card information.[6] Most of the remaining accounts in the top 500 belonged to Liberty Reserve exchangers.

*Aftermath of Liberty Reserve Shutdown*. Following the shutdown of Liberty Reserve in May 2013, law enforcement agents monitoring various online criminal forums (such as "hacking" or "carding" forums) observed numerous postings by users of these forums bemoaning Liberty Reserve's closure and the resulting loss of funds that they had on Liberty Reserve's system. Many users complained of losing tens of thousands of dollars or more that they had in their Liberty Reserve accounts.

By contrast, very few Liberty Reserve users have contacted the Southern District of New York seeking to recoup their Liberty Reserve funds on the basis that they were conducting legitimate business on the site. When the Liberty Reserve takedown was announced to the public in May 2013, users were instructed to contact the Southern District of New York if they wished to recoup their funds. Notwithstanding that Liberty Reserve had more than 5 million registered user accounts, *only 32 persons* have contacted the Southern District of New York from May 2013 to September 2014. Similarly, notwithstanding that numerous Liberty Reserve

[6] The accounts were categorized based on the account names and an examination of any websites they were associated with (which often had telltale phrases such as "cvv" or "hyip" in the account or website names).

accounts were doing a high volume of business as Liberty Reserve "exchangers," only one Liberty Reserve exchanger has contacted the Southern District of New York about a potential claim since May 2013, and that claim was ultimately not pursued.

Marmilev's Involvement in Liberty Reserve

Marmilev's history of involvement in Liberty Reserve dates back to 2003, when he was first hired to work for his co-defendants Arthur Budovsky and Vladimir Kats. At the time, Budovsky, Kats, and Marmilev all resided in Brooklyn, New York. Budovsky and Kats' primary online business then was a digital currency exchanger service named "GoldAge," which was a popular exchanger for "E-Gold" – then the most popular digital currency in operation. Starting in 2003, Marmilev worked for Budovsky and Kats; he administered the "GoldAge" website, and designed and administered websites for their various other online business ventures. These ventures included Liberty Reserve,– which Budovsky and Kats launched in or about 2002 as an alternative to "E-Gold," but which did not attract significant business until years later.

In or about January 2006, E-Gold's offices, which were based in the United States, were searched by federal law enforcement agents pursuant to a search warrant. The search was reported in the press and in online discussion forums followed by Budovsky, Kats, and Marmilev.

Six months later, in July 2006, while Marmilev was continuing to work for Budovsky and Kats, Budovsky and Kats were arrested for operating an unlicensed money transmitting business – GoldAge – in violation of New York state law. They were convicted in December 2006 and both sentenced to five years' probation. Following their convictions, Budovsky and Kats reverted to their prior conduct, continuing to operate another digital currency exchange and other digital currency-related businesses, and Marmilev, despite knowing that Budovsky and Kats had been arrested and convicted for operating GoldAge, continued to help them. For example, Marmilev helped operate an exchanger called Autocambist, placing advertisements for its services on HYIP forums.

In or about April 2007, E-Gold and several of its principals were indicted by the United States Attorney's Office for the District of Columbia on charges of money laundering and operating an unlicensed money transmitting business. The defendants pled guilty in or about July 2008. In particular, the founder of the company pled guilty to money laundering charges, based on evidence that the company was extensively used by online criminals (such as carding websites and HYIP Ponzi schemes) to launder the proceeds of their illegal activity. Again, these events were reported in the media and extensively discussed in online discussion forums followed by Budovsky, Kats, and Marmilev.

Notwithstanding the convictions of E-Gold and its principals, and notwithstanding their own convictions in connection with operating GoldAge, Budovsky and Kats set about building up Liberty Reserve as a successor to E-Gold, that would succeed in eluding law enforcement where E-Gold had failed, and would cater to the same customers who had been using E-Gold. By 2006, Budovsky and Kats had already incorporated Liberty Reserve in Costa Rica, with the idea of eventually moving the company's operations offshore. In or about 2007 and 2008, with Marmilev's help, Budovsky and Kats revamped the Liberty Reserve website and actively

marketed it to the same criminal constituencies that E-Gold had attracted. For example, according to a cooperating witness, Marmilev would open user accounts on HYIP-related websites and discussion forums, posing as an HYIP user, and offer testimonials praising Liberty Reserve's service. (Marmilev would also pay and recruit other Internet users to do so.) Notably, this information is corroborated by a password file recovered from Marmilev's computer during the investigation, which reflected usernames and passwords for various accounts Marmilev had on HYIP sites and discussion forums (such as "talkgold.com," "fastprofitsclub.com," "thewinterprofit.com," "game2money.com," and "captcha2cash.com") as well as usernames and passwords for carding forums (such as "verified.su," "blackvisa.info," and "carddomen.cn").

By 2009, Liberty Reserve had gained significant traction with HYIP websites and began doing a large volume of business. Around this time, Budovsky emigrated from the United States to Costa Rica, hired a staff of customer support representatives, and began running the company's operations from there.[7] Kats stayed behind in Brooklyn, but was forced out of the company by Budovsky by the end of 2009. Marmilev also stayed in Brooklyn, but, unlike Kats, he continued to be a key player in Liberty Reserve. Marmilev's work for Liberty Reserve included administering the company's website and maintaining its technical infrastructure, advising Budovsky regarding various matters related to the business, and supervising a staff of programmers located in the Ukraine as well as co-defendant Maxim Chukharev, who managed Liberty Reserve's local technological infrastructure in Costa Rica. In 2010, Marmilev was formally and knowingly made a part-owner of the company, with Budovsky giving him a 30% ownership share.

Marmilev also helped Budovsky run other digital currency businesses. In particular, from 2009 to 2013, Marmilev operated a Liberty Reserve exchange business, known as "ExchangeZone," in partnership with Budovsky. ExchangeZone facilitated over 17,000 exchange transactions, accounting for $10,776,090 in funds moved though the Liberty Reserve system.

Marmilev's Knowledge of the Illegal Nature of Liberty Reserve's Business

Marmilev was aware that Liberty Reserve's services were being used to process transactions for websites engaged in criminal activity, or he at least consciously avoided confirming the nature of websites using Liberty Reserve that were engaged in activity he knew was highly likely to be criminal.

As the person responsible for maintaining Liberty Reserve's technological infrastructure, Marmilev had unfettered access to all of the data on Liberty Reserve's transactional system – including the data described above clearly reflecting use of the system by criminal websites. Marmilev also was one of only two persons who had access to Liberty Reserve's Google Analytics account, which enabled him to view the referral data of the sort described above,

[7] While Budovsky actually controlled Liberty Reserve, he remained careful throughout not to have his name associated with the company. He used nominees to file corporate paperwork and open bank accounts, and portrayed himself simply as an "IT consultant" to the company's employees.

detailing the sources of traffic directed to Liberty Reserve's shopping cart interface. Indeed, extensive Liberty Reserve user data was found on Marmilev's laptop computer, which was searched during a border stop of Marmilev in early 2012. Thus, it was easily within Marmilev's grasp to inquire into the nature of the users of Liberty Reserve's system. And even with the limited data that Liberty Reserve collected about those users, it should have been obvious that many of the websites that accepted Liberty Reserve as payment were criminal in nature.

Moreover, as noted above, Marmilev was aware of the indictment and conviction of E-Gold and its principals for money laundering and operating an unlicensed money transmitting business, and knew of the underlying allegations that E-Gold was extensively used to launder criminal proceeds. Thus he knew the money-laundering dangers posed by a digital currency service that failed to implement effective know-your-customer and anti-money-laundering controls. Yet he continued to work with Budovsky and Kats in setting up and operating Liberty Reserve, knowing that it was designed to fill the very gap left by the demise of E-Gold and to cater to the same clientele.

Marmilev also had ample reason to doubt the integrity of Budovsky and Kats, given that they had been convicted for operating an unlicensed money transmitting business in 2006. Marmilev actively assisted Budovsky in concealing information about Budovsky's conviction. Specifically, in October 2009, Marmilev sent an e-mail to a "search engine optimization" or "SEO" expert, seeking to retain him to "clean up" search engine results for the search term "Arthur Budovsky." At issue were the "problems" posed by the press release on the Internet from the Manhattan District Attorney's Office concerning Budovsky's 2006 "indictment." Marmilev proposed that the SEO expert publish information on the Internet falsely suggesting that the "Arthur Budovsky" behind Liberty Reserve was a different person from the "Arthur Budovsky" who was convicted by the Manhattan District Attorney, but who simply happened to have the same name. Marmilev's evident purpose in doing so was to distance Liberty Reserve from Budovsky's criminal conviction, in an effort to promote an appearance of legitimacy for Liberty Reserve.

Marmilev also sought to conceal his own association with Liberty Reserve, failing to acknowledge his association with the company on certain occasions when called upon to provide his source of employment. Moreover, he consistently used aliases when conducting Liberty Reserve business. For example, in e-mails Marmilev sent to third-parties relating to Liberty Reserve business (such as correspondence with legitimate technology service providers, who he had no reason to fear would steal or misuse his true identity), he would sign them using an alias, such as "Marko Halls," "Mark Halls," "Michael Halls," and "Trent Halls."[8]

[8] Additionally, although Marmilev was made a 30% owner of the company in 2010, his ownership share was assigned to him in a confidential agreement and was never acknowledged in any public legal documents. For example, when Liberty Reserve identified its shareholders to Costa Rican regulators March of 2011, the company listed two nominees used by Budovsky, and failed to list either Budovsky or Marmilev as having any interests in the company.

Marmilev's Participation in Liberty Reserve's Deception of Regulators

Marmilev also participated in Liberty Reserve's efforts to deceive Costa Rican anti-money laundering regulators.

In or about 2008, Liberty Reserve embarked on the process of obtaining a money transmitting license from the Costa Rican agency known as the Superintendcia General de Entidades Financieras ("SUGEF"), a goal the company and its principals pursued until 2011. In March 2010, Liberty Reserve hired as its General Manager an experienced and well-respected Costa Rican banker named Marco Cubero, who Budovsky hired specifically to lobby SUGEF to approve a license for the company. One of SUGEF's requirements for a money transmitting license was that the company have an anti-money laundering ("AML") compliance officer. Accordingly, in November 2010, Cubero fulfilled that requirement by hiring an experienced Costa Rican banking professional named Sylvia Lopez.

Notwithstanding the hiring of Cubero and Lopez, Budovsky had no intention of implementing an effective AML program at Liberty Reserve. To the contrary, he, Marmilev, and other co-conspirators took actions designed to hide information about Liberty Reserve's users and the sources of its business from SUGEF, as well as the company's own General Manager and AML compliance officer, Cubero and Lopez. Specifically, in the late summer and fall of 2010, after SUGEF had advised that Liberty Reserve was required to have a system in place to monitor user accounts, Marmilev participated in a number of e-mail communications regarding the creation and implementation of a "Government Administrative Area (GAA)" on Liberty Reserve's computer system, where Cubero and Lopez could view statistics regarding Liberty Reserve accounts and transactions. Ostensibly, to the extent these statistics contained any suspicious information, Lopez would pass it on to SUGEF. However, the system was deliberately designed to ensure that Lopez would be given a limited and distorted view into Liberty Reserve's transactional database.

For instance, on June 24, 2010, Marmilev sent an e-mail to, among others, defendants Budovsky and Chukharev. The document set out the purpose and the function of the GAA. The GAA would allow the "Costa Rican government [to] view a few statistics," but the "[m]ajority of these statistics are going to be fake." The data displayed in the GAA would be manipulated by a Hidden Admin (HA) created by Marmilev and the other Liberty Reserve programmers. Once operational, Liberty Reserve would be able to use these systems to feed regulators fake statistics concerning the volume of transactions passing through Liberty Reserve and to hide account information for any specific accounts flagged in the HA.

Thereafter, on September 28, 2010, Marmilev sent an e-mail to Budovsky, Chukharev and another co-conspirator with the subject "GAA done," listing various final updates he made to the GAA. Marmilev noted in the email that he chose not to make a suggested update "in order to not provide an extra figure for sugef to check if the info is correct."

An October 26, 2010 e-mail communication between Marmilev and Budovsky indicates that the GAA was indeed intended to be reviewed by the company's AML compliance officer and the information passed on to SUGEF. On October 25, 2010, Marco Cubero sent Budovsky an e-mail asking him about the status of his request for a system to monitor user accounts, review

transaction reports and generate alarms that would satisfy SUGEF requirements. Cubero reminded Budovsky that this needed to be complete before the Compliance Officer, Sylvia Lopez, started on November 1, 2010. Budovsky forwarded this e-mail to Marmilev, who responded that a fully completed version of "the admins" was now operational.

Through the operation of the GAA/HA system, Budovsky and Marmilev tightly restricted the information available to Cubero and Lopez and, by extension, SUGEF, and fed them fake statistics that underreported the volume of transactions being processed by the company. However, despite their efforts, Liberty Reserve was not able to get a license from SUGEF. In March of 2011, Cubero resigned from Liberty Reserve, citing in part Liberty Reserve's failure to provide him with adequate reports on Liberty Reserve activity and Budovsky's refusal to allow him any access to the Liberty Reserve database. Lopez made similar complaints, going as far as to file the equivalent of a suspicious activity report ("SAR") against Liberty Reserve for its lack of adequate anti-money laundering controls.

Marmilev's Proceeds from Liberty Reserve

As noted, in 2010, Marmilev became a 30% owner of Liberty Reserve, but he received substantial profits from Liberty Reserve even before becoming an owner. Starting in 2009, Budovsky wired Marmilev $1.3 million in Liberty Reserve-derived funds that Marmilev used to renovate and purchase equipment for a store he owned in Brooklyn called "Gourmet Boutique" that he ran with the help of his aunt, Yanina Izraitel. Through Gourmet Boutique, Marmilev paid himself a salary of $2,000 per week that he took in cash. He received an additional $300,000 from Budovsky that he used for renovations for other Brooklyn-based businesses he owned. The $1.3 million payment was categorized as a loan for accounting purposes, but none of the monies he received from Budovsky were ever repaid.[9]

A full accounting by the Government of how much money Marmilev made from his involvement in Liberty Reserve is not possible. At times, Marmilev received Liberty Reserve-connected funds from third-party sources in ways that obfuscate the source of the funds received. In addition, Budovsky sent LR to Marmilev through Liberty Reserve accounts to which Marmilev had access. Marmilev could easily have converted the LR to mainstream currency he could keep for himself by selling the LR to his Autocambist or ExchangeZone customers. The extent to which Marmilev received funds through this method is unknown.

[9] Marmilev repeatedly sought to hide his association with Gourmet Boutique in light of its connection to Liberty Reserve. For example, as noted above, on January 13, 2012, Customs and Border Protection (CBP) and Homeland Security Investigations (HSI) agents conducted an inbound border inspection of Marmilev and his personal effects, including his laptop computer and other electronic devices. Soon after that inspection took place, Marmilev conducted a sham transfer of ownership of both of his businesses to Yanina Izraitel. The documents were back-dated to show 2011 execution dates, even though the metadata for the transfer document indicates the agreement was created in 2012. During an outbound inspection in 2013, Marmilev told CBP that he was an information technology "contractor" and that Gourmet Boutique was one of his "clients."

Without regard to how he received funds, Marmilev's lifestyle reflected a substantial regular income. He drove a $42,000 Audi luxury sedan and he engaged in significant international travel. Marmilev took nine international trips between 2010 and 2013, visiting Costa Rica three times, Russia and Israel twice each, and Canada and France once, respectively.

## DISCUSSION

### I. A Guidelines Sentence Is Warranted Based on the Enormous Volume of Transactions Processed by Liberty Reserve as an Unlicensed Money Transmitting Business

It is undisputed that Liberty Reserve did business with United States customers throughout its operation, encompassing hundreds of millions of dollars in transactions, yet it never registered as a money transmitting business with the U.S. Department of Treasury. Marmilev also does not dispute that he helped operate the business for years while knowing it was unregistered with U.S. authorities, even though he knew that other digital currency businesses (including ones he had helped operate) had been prosecuted by U.S. authorities for failing to register under federal law. For these reasons alone – putting aside Marmilev's level of knowledge as to the criminal proceeds being moved through the business, which is addressed below – a Guidelines sentence is warranted.

As he must, Marmilev acknowledges that the Guidelines calculation included in his plea agreement as to his participation in a conspiracy to violate 18 U.S.C. §1960(b)(1)(B) applied the appropriate section of the Sentencing Guidelines. (Mem. at 8-9). He also concedes that the sentencing range advised by the Guidelines – incorporating a 28-point increase in his offense level because between $200 million and $400 million was transmitted by Liberty Reserve to, from, or on behalf of U.S. users – was properly calculated. (*Id.*). Because his sentencing exposure is effectively capped at 60 months by the statutory maximum, Marmilev has already received considerable relief from this 28-point increase. Nonetheless, Marmilev argues that a Guidelines sentence of 60 months is still unwarranted, contending that his crime was "[p]rimarily a [l]icensing [v]iolation" and a "strict liability offense," (*id.* at 8-9), and that it would be unjust to sentence him "in the same range as an offender who steals, defrauds, or willfully structures transactions involving funds exceeding $200 Million." (*Id.* at 10).

Marmilev cites no authority for his position except for a lone dissenting opinion in a D.C. Circuit case. (Mem. at 9-10 (citing *United States v. Keleta*, 552 F.3d 861, 867-68 (D.C. Cir.) (Williams, J., dissenting)). Marmilev's reliance on the dissent in *Keleta* is unavailing, however, primarily because the dissent suggests that Section 1960 violations pose little risk to the financial system despite clear authority indicating otherwise. The Second Circuit has specifically observed that "Title 18 U.S.C. § 1960 was enacted in order to combat the growing use of money transmitting businesses to transfer large amounts of the monetary proceeds of unlawful enterprises." *United States v. Velastegui*, 199 F.3d 590, 593 (2d Cir. 1999) (citing S. Rep. No. 101–460, at 14 (1990), *reprinted in* 1990 U.S.C.C.A.N. 6645, 6658–59). The Senate Report cited in *Velastegui* highlights testimony noting that "[i]t is primarily the unlicensed money transmitter that provides the best means of laundering money and is most often used to structure illegal transactions." S. Rep. No. 101–460, at 14 (1990), *reprinted in* 1990 U.S.C.C.A.N. 6645,

6658–59. As another court put it when applying an 18-level enhancement in a Section 1960 case based purely on the volume of funds processed by the business, "[t]he more money that is transmitted by an unlicensed business, the more likely that some of that money will find its way into criminal hands, and hence, the greater the harm caused." *United States v. Bariek*, No. 05 Cr. 150 (JCC), 2005 WL 2334682, at *2 (E.D. Va. Sept. 23, 2005).

Accordingly, neither Congress nor other courts, including the majority in *Keleta*, consider those who violate Section 1960 to be participating in low-risk behavior. Particularly here, where the unlicensed money transmitting business at issue transmitted, at a minimum, hundreds of millions of dollars tied to U.S. customers, the anti-money laundering policies underlying Section 1960's enactment were contravened to a far greater degree than in the more typical, smaller-scale Section 1960 case. Marmilev's sentence should reflect that disparity as part of the greater seriousness of his offense.

Nor should Marmilev receive any lenient treatment based on the notion that he was unaware of U.S. licensing requirements and is only guilty of violating Section 1960 on a "strict liability" theory. This is not a case where the failure to register was due to mistake or ignorance of the law. Liberty Reserve's founders, Budovsky and Kats, moved the company to Costa Rica specifically to avoid U.S. jurisdiction, because they knew that Liberty Reserve's predecessor, E-Gold, had been shut down as an unlawful money transmitting business, and because they themselves had been convicted for operating an E-Gold exchange service (which Marmilev helped operate as well) as an unlicensed money transmitting business. Marmilev, a longtime associate of Budovsky and Kats, was well aware of these law enforcement actions and well aware of the reason for moving Liberty Reserve offshore. Indeed, on Liberty Reserve's own webpage (which Marmilev maintained), the company favorably advertised its offshore status, specifically comparing itself to Paypal and other U.S. based payment services on the ground that the "[a]dministration and bank accounts" of those services were "under US jurisdiction." (*See* Ex. F (screenshot of promotional chart comparing Liberty Reserve to other payment processors)). Further, as detailed below, Marmilev himself marketed Liberty Reserve to users on Internet discussion forums by promoting the impression that Liberty Reserve was untouchable by U.S. law enforcement.

Accordingly, Liberty Reserve's failure to register was part of a deliberate attempt to escape any monitoring by U.S. authorities and any obligation to comply with U.S. anti-money laundering requirements – even though the company did business with U.S. customers throughout its operation. Nor does Marmilev ultimately dispute this fact, even though he characterizes it differently (and incorrectly): he admits that Liberty Reserve moved to Costa Rica "because it learned from the example of predecessor businesses – in particular E-Gold – that the United States is hostile to virtual currencies." (Mem. 27). Thus, Marmilev cannot seriously contest that he was aware that digital currency businesses such as Liberty Reserve were required to register as money transmitting businesses under U.S. laws and he knew that Liberty Reserve deliberately sought to avoid the reach of those laws by moving its operations outside the United States.[10]

[10] In his sentencing submission, Marmilev argues that it was not clear that Liberty Reserve qualified as a money transmitting business under U.S. law until the U.S. Department of

In short, there is no dispute between the parties that Liberty Reserve moved hundreds of millions of dollars belonging to U.S. customers without registering as a money transmitting business under U.S. law. Nor is there any dispute that Liberty Reserve's principals, including Marmilev, were well aware that U.S. authorities considered digital currencies to be money transmitting businesses and believed them to pose serious money-laundering dangers. Based on these undisputed facts alone, a Guidelines sentence is warranted.

The sentencing outcome in the *E-Gold* case does not counsel to the contrary. Marmilev points to the fact that the highest sentence imposed in that case was 14 months. But the very fact that Marmilev was evidently not deterred by the sentences imposed in *E-Gold* supports the imposition of a much firmer sentence in this case. Again, instead of abandoning the E-Gold model after it was shut down and attempting to operate a digital currency business that complied with federal anti-money laundering laws, Marmilev and his co-conspirators moved the company to Costa Rica to evade those laws and attempt to avoid the same fate that had befallen E-Gold. Their reaction suggests that the sentences in that case were too lenient to deter similar criminal conduct. Thus, contrary to Marmilev's assertion that his sentence should mirror that of the E-Gold defendants, (Mem. at 37), a sentence in line with the stipulated Guidelines range in this case, as recommended by Probation, is warranted to ensure adequate specific and general deterrence.

## II. A Guidelines Sentence Is Further Warranted Based on the Extensive Criminal Use of Liberty Reserve and Marmilev's Awareness Thereof

In addition to pleading guilty to 18 U.S.C. § 1960(b)(1)(B) – the failure to register offense – Marmilev also pled guilty to 18 U.S.C. § 1960(b)(1)(C) – operating a money transmitting business involving funds known to the defendant to have been derived from or to be intended to promote criminal activity. Marmilev specifically admitted during his plea allocution that he believed that a "substantial amount" of the funds moving through Liberty Reserve from the United States came from so-called "high yield investment programs" (or "HYIPs") that he believed "had a high probability of being fraudulent," but he "consciously avoided obtaining confirmation" of that fact. Given that the parties agree that the funds moving through Liberty Reserve from the United States amounted to hundreds of millions of dollars, this admission alone provides an independent basis for imposition of the 60-month sentence called for under the stipulated Guidelines analysis. Even if only ten percent of the funds at issue came from HYIPs, the implication would be that Marmilev willfully turned a blind eye to more than $20 million in proceeds of wire fraud that were processed through his company's system. Under the Guidelines

---

Treasury's Financial Crimes Enforcement Network ("FinCEN") issued certain guidance concerning digital currencies in March 2013. However, given Marmilev's familiarity with the E-Gold prosecution, he was aware that digital currency services were subject to the federal laws governing money transmitting businesses, including Section 1960, well before the issuance of FinCEN's March 2013 guidance, which merely clarified certain existing FinCEN regulatory requirements and did not announce any new law.

provision specifically applicable to violations of 18 U.S.C. § 1960(b)(1)(C), the advisory range would be 70 to 87 months – with a plea – based on laundered funds of that amount.[11]

In his sentencing submission, Marmilev now seeks to downplay the extent of his knowledge of the criminal proceeds moving through Liberty Reserve. But he does not disavow his plea allocution. And moreover, although the Court need not resolve the issue in this context, there are clear facts, which Marmilev cannot seriously dispute, confirming that online criminal enterprises were a major driver of Liberty Reserve's business, and that Marmilev knew it.

### A. Criminal Use of Liberty Reserve Was Extensive

As the statistics set forth in the factual background above make clear, Liberty Reserve was not a mainstream payment processor that simply happened to be used occasionally by criminals. *Thousands* of criminal websites relied on Liberty Reserve as their payment processor of choice. These websites predominated the sources of Liberty Reserve's online traffic and generated *billions* of dollars in transactions run through the company's system. Liberty Reserve depended on these websites to sustain its business.

Marmilev's attempts to minimize the significance of Liberty Reserve's criminal clientele are wholly unpersuasive. For example, Marmilev dismisses the fact that Liberty Reserve's Google Analytics data reflects at least 1,300 credit card-trafficking websites with "card" or "cvv" in their names that used Liberty Reserve to process transactions, arguing that the Liberty Reserve accounts associated with these websites constituted an "infinitesimally small" portion of Liberty Reserve's 5.1 million user accounts. However, this argument ignores that the accounts in question were accounts of "merchants" rather than individual users, and as such they would have generated a much greater volume of business compared to individual user accounts. (Moreover, for each "merchant" account associated with a criminal enterprise, there would have been hundreds or thousands of individual Liberty Reserve users who used the service to transfer money to these criminal enterprises.) As explained above, an examination of Liberty Reserve's top 500 accounts showed that credit card-trafficking sites alone (putting aside other types of criminal websites) accounted for approximately $210 million in transactions processed through Liberty Reserve – hardly an "infinitesimal" sum.

Nor can Marmilev credibly argue that the criminality of the websites using Liberty Reserve is difficult to discern. Marmilev argues that the mere fact that a Liberty Reserve account name or associated website contained terms such as "cvv," "card," or "HYIP," is not conclusive evidence that the operator of the account was engaged in criminal activity. Perhaps it is not conclusive evidence, but it is a pretty obvious hint – one that would, for example, lead an diligent bank employee to raise compliance questions or file a Suspicious Activity Report. It does not require extended detective work to conclude that a Liberty Reserve account associated with a username such as "isellcvv" or a website address such as "icarder.ru" is likely selling

[11] The plea agreement between the parties is based instead on U.S.S.G. § 2S1.3, which applies specifically to the 18 U.S.C. §1960(b)(1)(B) offense, *i.e.*, the registration offense, and which turns on the total amount of funds passed through the business rather than only the portion tied to criminal activity.

stolen credit card information, or that a Liberty Reserve account explicitly associated with the term "hyip" is likely peddling a so-called "high-yield investment program."

In any event, the Government's analysis is not based on a survey of account names or website addresses alone; from simply visiting many of the websites referring traffic to Liberty Reserve, the criminal nature of the websites is readily apparent. For example, one of the top traffic-generating websites reflected in Liberty Reserve's Google Analytics data is a website known as "validshop.su." Not only is this website known to be a carding site from independent law enforcement investigation, but the website on its face, at the time of Liberty Reserve's operation, bore obvious indicia of illegal carding activity. For example, the site's "terms and conditions," which were visible to the public, stated that "Cvvs Can Be Checked Right Before Sell At Customers Wish At Additional Price" and that replacements are available if a check shows the "CCNUM+EXP" is "not APPROVED." (*See* Ex. G (screenshot)).

Similarly, HYIP-style Ponzi schemes are typically easy to discern, based on their unexplained promises of impossible profits, and their insistence on receiving investments in the form of Liberty Reserve or other anonymous digital currencies with "no chargeback" policies in the event a customer complains of being defrauded. Several examples of HYIP sites listed among the top 20 traffic-generating sites in Liberty Reserve's Google Analytics data are attached as Exhibit H, and illustrate the point. One, for instance, "justbeenpaid.com," promises users the ability to "Earn 2% per Day or 60% per Month" and "Use Daily Compounding to Increase Your Earnings." (Ex. H). Another, "royalty7.com," promises an "amazing 154% monthly ROI [return on investment] over the long term." (*Id.*). A third, "profitclicking.com," promises users they can "Start with Just $10 and Turn It into a Fortune"; all they have to do, the site indicates, is "Click on three websites a day and Receive Your Generous Daily Commissions." (*Id.*). At the very least, any person of reasonable sophistication would realize, as Marmilev admits he did, that such websites had a "high probability of being fraudulent."

### B. Marmilev Knew That Criminal Use of Liberty Reserve Was Extensive

In fact, Marmilev knew that carding and HYIP websites, among other criminal enterprises, were a key part of Liberty Reserve's clientele. As to HYIP sites in particular, Marmilev not only knew they were important clients; he specifically promoted Liberty Reserve on HYIP discussion forums. These forums are often frequented by administrators of HYIP sites, as well as Internet users who are aware that HYIP sites are mere Ponzi schemes but who attempt to monitor and "gamble" on the schemes before they implode. Marmilev posted extensively on these forums to advertise features of Liberty Reserve that would appeal to this audience – including its lack of customer verification policies and its location supposedly outside the reach of U.S. authorities.

Although Marmilev denies this allegation, (Mem. at 38), the denial is demonstrably false. Marmilev's computer, which was searched in the course of the investigation, was found to contain a "Roboform" file, a type of password-manager file containing login credentials for websites, which the "Roboform" application automatically fills in upon visiting any website for which credentials are stored. Included in the file on Marmilev's computer were login credentials to various HYIP discussion forums – including login credentials for the usernames "Redd" and

"vintage" on an HYIP discussion forum known as "talkgold.com." (*See* Ex. I (excerpts from password file)). Marmilev used these accounts to make numerous comments on "talkgold.com" in which he vouched for Liberty Reserve (along with other digital currency businesses that Marmilev helped Budovsky and Kats operate), and assured users on the HYIP forum that their money would be safe at Liberty Reserve. For example:

- In one post, dated December 15, 2009, "Redd" responded to a question from another forum user asking whether Liberty Reserve or WebMoney ("WMZ") – a Liberty Reserve competitor – had ever "blocked an account . . . only for the main reason that it had over 10k in it and was unverified." "Redd" responded that he had once had more than $10,000 in a WebMoney account from a "questionable" source and that WebMoney had "asked for more info" about it. By contrast, "Redd" stated that he had "[n]ever had any problems with any amounts" with Liberty Reserve, adding that "*LR is much more tolerant towards shady businesses than [Webmoney]*." (Ex. J) (emphasis added).

- In another post, from November 2008, "vintage" responded to a forum user who worried that if LR "continue[d] to support scams like HYIPs and other fishy businesses which are advertised on Talkgold" then the company might be shut down "like e-gold.com," and suggested that any payment system seeking to avoid such an outcome "should ask about an ID." The user asked others on the forum whether they agreed: "Don't you think so?" "Vintage" answered the question, "Nope," and commented that "[o]nly those payments systems that are in [the] US" had to ask customers for their IDs. (Ex. K).

- In another post, from October 2007, "Redd" responded to a user falsely claiming that Liberty Reserve had been "raided by Costa Rican authorities" at the time. "Redd" stated that the story was a "fake" and that "Costa Rica and USA do NOT have an MLAT (Mutual Legal Assistance Treaty) agreement between them. But PANAMA DOES!!!!" Pointing to competitors of Liberty Reserve that claimed to have offices in Panama, "Redd" warned other users to avoid those services, stating: "I do not want to lose funds in any currency that can be shut down by USGov." (Ex. L).

- "Redd's" posts also make clear that Marmilev suffered from no illusions about the fraudulent nature of HYIPs. For example, in one post in a discussion thread about an "Internet Fraud Complaint Center" established by the FBI (Ex. M), "Redd" commented:

  > People just don't understand that HYIP is a synonym for Gambling. . . . Don't read the bull**** stories these hyips give you. The rules are simple:
  > 1. give us your money
  > 2. wait a few cycles.
  > 3. withdraw your money before we close.
  > There are more advanced guidelines on how to increase your chances in hyip, but that's a secret ☺

Thus, Marmilev – in his own words – has fully acknowledged the criminality of HYIPs, and went so far as to promote Liberty Reserve to HYIP operators based on its lax enforcement and purported insulation from the reach of U.S. authorities.

There is every reason to believe that Marmilev knew that Liberty Reserve's business was fueled by criminal sources other than HYIPs as well, such as credit card-trafficking sites. As noted above, Marmilev was only one of two persons who had access to Liberty Reserve's Google Analytics data, the very purpose of which is to track the sources referring traffic to a business's website. It is not credible that Marmilev would simply never have bothered to notice that many of the sites generating the largest number of referrals to Liberty Reserve were carding sites. Indeed, the fact that Marmilev had login credentials for carding sites as well on his Roboform file indicates at a minimum that he was aware of the existence of such sites and their use of Liberty Reserve.[12]

While Marmilev claims to have no "specific knowledge" of how much of Liberty Reserve's business was criminal in nature, (Def.'s Mem. at 15), there is no need for the Government to establish, or for the Court to determine, any such specific figure for purposes of sentencing.[13] What matters is that Marmilev helped operate Liberty Reserve for years while knowing that fraudulent and criminal websites were major drivers of the business's revenue. A Guidelines sentence of 60 months is amply warranted for this reason.

### C. Liberty Reserve Lacked Any *Bona Fide* AML Compliance Program

As Marmilev's posts on talkgold.com indicate, Liberty Reserve set up in Costa Rica in order to avoid the scrutiny of U.S. law enforcement. *See also* PSR ¶51. Although the Court need not resolve the issue, Marmilev's contentions that Liberty Reserve nonetheless "employed anti-money laundering procedures that are virtually identical to those required in the U.S." amount to sheer fancy on his part. The evidence instead shows that Liberty Reserve's purported AML procedures were a fig leaf designed to hide the fact that the company lacked any serious program designed to prevent criminals from using Liberty Reserve and to report suspicious activity to law enforcement authorities. *See* PSR ¶¶61-62.

---

[12] Marmilev contends that he had such login credentials only to investigate phishing fraud he suspected these websites of perpetrating: *i.e.*, he suspected that, when users were being prompted to pay for purchases on the sites, the sites were directing them to a phony version of Liberty Reserve's website in order to induce them to enter their Liberty Reserve login credentials, for the purpose of later hacking into their accounts. Even if true, such incidents would surely have put Marmilev on notice of the use of Liberty Reserve by websites trafficking in stolen credit card data.

[13] Indeed, to the extent there is uncertainty, the Guidelines counsel that the uncertainty is to be resolved in favor of the Government. Under U.S.S.G. § 2S1.1 – the guideline applicable to violations of 18 U.S.C. § 1960(b)(1)(B) –where "legitimately derived funds" are commingled with "criminally derived funds," the burden is on the defendant to "provide[] sufficient information to determine the amount of criminally derived funds without unduly complicating or prolonging the sentencing process." Otherwise, "the value of the laundered funds" is the "total amount of the commingled funds." U.S.S.G. § 2S1.1, application note 3(B).

At a very basic level, Liberty Reserve's AML policies were meaningless because Liberty Reserve intentionally failed to verify the identities of its users, opting instead to classify only a handful of Liberty Reserve *exchangers* as the company's "customers," while ignoring the company's actual end users. *See* Ex. N, Letter from Jafet Zuniga Salas and Cecilia Sancho Calvo to Allan Hidalgo dated July 21, 2011. To avoid having to verify the identity of users and having to learn the true origin and destination of the funds going through Liberty Reserve, the company sought to absolve itself from any liability for criminal use of the system by its users by taking the position that Liberty Reserve exchangers were responsible for AML compliance with respect to end users, even though exchangers had no visibility into user activity within Liberty Reserve's system. (*Id.* at 1). Although SUGEF (Costa Rica's financial superintendent) made it clear that such a policy was not acceptable, and that Liberty Reserve was itself responsible for verifying the identity of users and tracking the sources and uses of funds going through its own system, (*id.* at 3-4), there is no evidence Liberty Reserve ever changed its policy. Indeed, law enforcement was able to conduct undercover transactions on the Liberty Reserve website worth $12,000 without encountering any attempt to collect verification information – either by the exchangers involved or by Liberty Reserve itself.

Moreover, the evidence shows that Liberty Reserve's principals did not even take the verification of exchangers seriously. For example, one of Liberty Reserve's primary exchangers was Swiftexchanger, an exchange service secretly owned by Budovsky and Liberty Reserve co-conspirator Azzeddine El Amine and operated by El Amine. PSR at ¶¶18, 22. In seeking to hide the fact of his ownership of the company, Budovsky submitted false documentation to Liberty Reserve's own verifications department, which was forwarded to SUGEF. Specifically, at the end of February 2011, Budovsky sent an e-mail to El Amine attaching identity documents in the name of "Anatoly Gursky," which Budovsky instructed El Amine to use to update El Amine's "profile." (*See* Ex. O (February 28, 2011 E-mail from Arthur Budovsky, using the address redghost@150mail.com, to Azzeddine El Amine)). About two days later, the Swiftexchanger "management" sent these identity documents to Liberty Reserve's verifications department via email, with the subject line "Documents for Verification." (*See* Ex. P (e-mail from Management@swiftexchanger.com to exchangers@libertyreserve.com dated March 2, 2011)). This false documentation was subsequently forwarded to SUGEF in November of 2011, in response to a request by SUGEF for information about the identities of Liberty Reserve's "clients." (*See* Ex. Q (Letter from Allan Hidalgo to Nidia Varela dated November 24, 2011 (listing Swiftexchanger as a "client" of Liberty Reserve controlled by "Anatoly Gursky" and based in Germany)). This act of deception by Liberty Reserve's own founder underscores how the company's "verification" policy was a sham.

Marmilev, too, participated in deceiving SUGEF and Liberty Reserve's compliance staff. As the PSR explains, Marmilev and his co-conspirators devised a system to provide false statistics to and hide account information from Liberty Reserve's compliance officer, Sylvia Lopez, and SUGEF. PSR ¶¶62-66. While Marmilev asserts that Liberty Reserve used these administrative areas to underreport Liberty Reserve's transactions in order to avoid taxation, (Mem. at 31), Liberty Reserve's internal emails make it clear that the fake statistics were intended to be seen by the compliance officer and SUGEF, neither of whom had anything to do with Liberty Reserve's taxes. But even if Marmilev's claim were true, the fact that he

participated in creating an elaborate, hidden system specifically designed to deceive Liberty Reserve's own compliance officer – about *any* aspect of Liberty Reserve's business – hardly instills confidence in the integrity of Liberty Reserve's supposed AML program. To the contrary, it shows that Marmilev (along with his co-conspirators) regarded Liberty Reserve's AML compliance officer as an outsider who needed to be kept at bay and did not see a particular need for honesty and transparency in dealing with her.

In any event, it is indisputable that starting in November 2011 -- after Liberty Reserve withdrew its application for a license from SUGEF, fired its compliance officer, and purported to close its offices in Costa Rica -- the company had no AML compliance program whatsoever. Yet the company continued to operate until May 2013, when it was shuttered by U.S. and Costa Rican law enforcement. Marmilev thus is hard pressed to explain how Liberty Reserve is supposed to have been AML compliant during this one-and-a-half-year time period. He does not address this issue in his memorandum, except to blame U.S. anti-money laundering authorities, *viz.*, FinCEN, for Liberty Reserve's inability to operate in Costa Rica after November 2011, as a result of the notice FinCEN provided to Costa Rican authorities around this time concerning suspected money laundering by Liberty Reserve. But FinCEN's notice did not preclude Liberty Reserve from working with SUGEF or other authorities to create a viable anti-money laundering program. Instead, Liberty Reserve unilaterally terminated its application for a license in Costa Rica and falsely told SUGEF the company was being sold to a company based in Cyprus. *See* Ex. R at 1-2, Letter from Allan Hidalgo to the SUGEF General Financial Institution Oversight Commission dated November 28, 2011.[14] Apparently, Liberty Reserve's principals once again made evasion of scrutiny by U.S. authorities a higher priority than adopting serious AML controls.

The only meaningful compliance to which Marmilev can point in his memorandum consists of a single instance when Liberty Reserve's compliance officer answered an inquiry from an FBI agent for information about a Liberty Reserve account. It is unsurprising that Liberty Reserve's compliance officer chose not to ignore a law enforcement request. But this isolated effort hardly makes up for the profound deficiencies in Liberty Reserve's AML program. Because of the company's lack of know-your-customer requirements for its end users, any account information it had available to provide to law enforcement was unverified. Moreover, because Liberty Reserve lacked any policy of determining the types of businesses operating on its system, the company failed to detect suspicious activity on its own in order to *report* the activity *to* law enforcement and take other appropriate action.[15]

---

[14] While Marmilev suggests that Liberty Reserve was in fact moved to Cyprus, the sale was a sham that merely involved moving the company's shares to a Cyprus shell company held in the name of Azzeddine El Amine and the company's funds to a Cyprus-based bank account. Liberty Reserve never operated in Cyprus, however, and by the end of February 2012, all the funds in the account in Cyprus had been moved to Russia.

[15] Marmilev claims that Liberty Reserve "froze approximately 5,000 accounts suspected of unlawful conduct," (Mem. at 30), but Marmilev has not produced the spreadsheet on which this assertion is base, and therefore the Government cannot test it. More significantly, the Government has seen no evidence that any such accounts were ever reported by Liberty Reserve to any law enforcement authorities, or that Liberty Reserve returned any funds involved to

Ultimately, however, the extent of Liberty Reserve's AML compliance efforts is not an issue that the Court need resolve. The pervasive criminal use of Liberty Reserve demonstrates that those efforts were woefully inadequate. Again, as explained above, Marmilev knew – or had strong reason to know – that Liberty Reserve was extensively used by criminals, and for this reason alone a Guidelines sentence is well justified.

## CONCLUSION

For the reasons set forth above, the Court should impose a Guidelines sentence of 60 months' imprisonment, consistent with the recommendation made by Probation and the principles of sentencing set forth in 18 U.S.C. § 3553(a). Marmilev (a) helped operate a business that transmitted hundreds of millions of dollars associated with U.S. customers without obtaining a federal money transmitting license, despite having been involved in a similarly unlawful company that was shut down by law enforcement; and (b) knew from the outset that the business involved transmitting substantial amounts of criminal funds. Either one of these fundamental facts – which are not meaningfully contested by Marmilev and which are encompassed by his plea allocution – provides a sufficient basis for imposition of the sentence called for under the Guidelines. Indeed, as noted by Probation, Marmilev has already received considerable favorable treatment in that his sentence is statutorily capped at 60 months, whereas otherwise he would face more than double that amount of exposure under the Guidelines (135 to 168 months). Particularly in light of that circumstance, a 60-month sentence is appropriate, as anything less would fail to reflect the seriousness of the offense and to provide adequate deterrence against similar conduct.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: /s/ Serrin Turner
SERRIN TURNER
ANDREW D. GOLDSTEIN
CHRISTINE I. MAGDO
KEVIN MOSLEY
Assistant United States Attorneys

cc: Seth Ginsberg, Esq. (by ECF)

---

defrauded parties. Indeed, Liberty Reserve had an explicit policy of "no chargebacks" in response to complaints from users who reported being defrauded. Thus, to the extent Liberty Reserve did block any user accounts, the company presumably kept the money for itself.